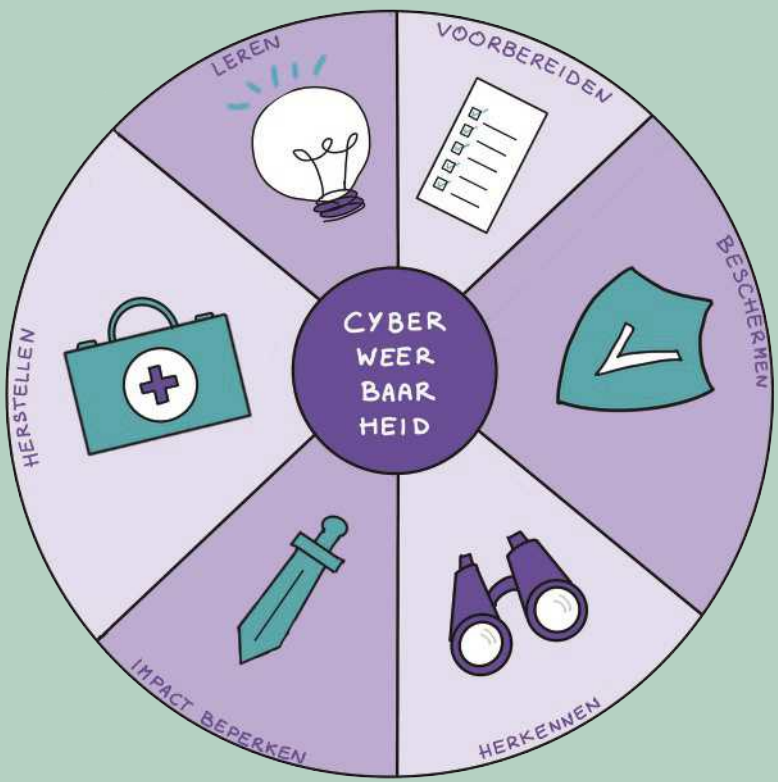
1


LEREN
VOORBEREIDEN
BESCHERMEN
HERKENNEN
IMPACT BEPERKEN
HERSTELLEN
CYBER
WEER
BAAR
HEID

INLEIDING

Rutger Leukfeldt, Carlyn van Amersfoort, Remco Spithoven, Jurjen Jansen

1.1 OVER CYBERWEERBAAR NL EN DE ONDERZOEKSAGENDA

Online criminaliteit is al jaren onderwerp van onderzoek. Toch wordt dit onderzoek door professionals ervaren als gefragmenteerd en te weinig aangesloten op de praktijk. Het expertisenetwerk Cyberweerbaar NL wil bestaande inzichten bundelen en samen met praktijkpartners nieuwe, hoogwaardige kennis ontwikkelen. Van welke thema's weten we al het nodige en van welke thema's nog nagenoeg niets? Op welke onderwerpen hebben we in Nederland al expertise en wat zijn de grootste uitdagingen de komende jaren? Deze onderzoeksagenda laat zien op welke thema's de kennisinstellingen binnen Cyberweerbaar NL zich richten. De onderzoeksvragen die in ieder thema zijn geformuleerd dienen als een concrete aanzet om het cyberweerbaarheidsdomein verder te brengen. Dit betreft zeker geen uitputtende lijst. Samen met alle praktijkpartners gaan we aan de slag om gezamenlijk te bepalen welke thema's we de komende jaren verder uitdiepen en welke onderzoeksvragen daarbij prioriteit moeten krijgen. Deze onderzoeksagenda is daarmee een vertrekpunt.

Deze onderzoeksagenda gaat in op vijf hoofdthema's. Hoofdstuk 2 bespreekt de slachtofferkant van online criminaliteit, zoals de omvang en de risicofactoren. Hoofdstuk 3 behandelt gedrag en gedragsverandering, bijvoorbeeld effectieve risicocommunicatie. Hoofdstuk 4 gaat in op het versterken van de cyberweerbaarheid aan de publieke kant. Hoofdstuk 5 bespreekt het versterken van de cyberweerbaarheid aan de

private kant, zoals *incident response* bij het mkb. Als laatste behandelt hoofdstuk 6 de daders van online criminaliteit, waaronder de ontwikkelpaden van cybercriminelen en cybercrime-as-a-service. Hoewel we hebben getracht overlap te voorkomen, kan het zijn dat een enkel onderwerp vanuit verschillende perspectieven aan bod komt. Voordat we overgaan tot de onderzoeksthema's, gaan we eerst dieper in op wat wij verstaan onder cyberweerbaarheid (par. 1.2), online criminaliteit (par. 1.3) en effectieve aanpakken en interventies (par. 1.4).

1.2 OVER CYBERWEERBAARHEID

In de nationale cybersecuritystrategie 2022-2028 (NCSC, 2022, p. 9) wordt cyberweerbaarheid gedefinieerd als:

> 'het vermogen om (relevante) risico's tot een aanvaardbaar niveau te reduceren door middel van een verzameling van maatregelen om cyberincidenten te voorkomen en wanneer cyberincidenten zich hebben voorgedaan deze te ontdekken, schade te beperken en herstel eenvoudiger te maken'.

In de (internationale) literatuur wordt cyberweerbaarheid op verschillende wijzen gedefinieerd. Eén die aansluit op de bovenstaande definitie en daarbij de doelstelling van cyberweerbaarheid verduidelijkt, is die van Dupont et al. (2023, p. 3, gebaseerd op Björk et al. [2015] en Linkov & Kott [2019]):

> '[T]he ability to prepare, absorb, recover, and adapt to adverse effects caused by cyberattacks […], with the ultimate aim for the organization to continuously deliver the intended functions or services.'

1.3 OVER ONLINE CRIMINALITEIT

Voor criminaliteit waarbij technologie van wezenlijk belang is voor de uitvoering ervan bestaan verschillende benamingen

en categorieën. In het huidige criminologische onderzoek naar online criminaliteit worden in de regel twee categorieën gebruikt. De gangbare Engelse terminologie van deze categorieën is *cyber dependent crime* en *cyber enabled crime* (McGuire & Dowling, 2013; Beerthuizen et al., 2020). In het Nederlands kan dit vertaald worden als 'cybercriminaliteit' en 'gedigitaliseerde criminaliteit'. Beide categorieën en hun mengvormen vallen onder het paraplubegrip 'online criminaliteit'.

Delicten die vallen onder de noemer cybercriminaliteit kunnen worden gezien als 'nieuwe' vormen van criminaliteit. Immers, ICT is in dit geval niet alleen een middel om het delict te plegen, maar ook het doelwit. Dergelijke delicten waren in het pre-digitale tijdperk simpelweg niet mogelijk, omdat er nog geen ICT-infrastructuur was om aan te vallen. Voorbeelden zijn hacken (het zonder toestemming binnendringen in een geautomatiseerd werk), het gebruik van malware (kwaadaardige software zoals een virus of spyware), ransomware (het versleutelen van digitale informatie of systemen en daar losgeld voor vragen), DDoS-aanvallen (het platleggen van een digitaal systeem door deze te overbelasten) en *defacen* (het zonder toestemming aanpassen van websites).

Delicten die vallen onder de noemer 'gedigitaliseerde criminaliteit' zijn feitelijk delicten die er in het pre-digitale tijdperk ook al waren, maar waarbij ICT nu van wezenlijk belang is voor de uitvoering van die delicten. Een voorbeeld is het uitvoeren van een phishingcampagne, waarbij criminelen via een valse e-mail proberen inloggegevens van mensen te ontfutselen om zo controle te krijgen over de online bankieromgeving van slachtoffers. Vervolgens is het doel om geld via zogenaamde geldezels over te sluizen van de rekening van een slachtoffer naar rekeningen van de criminelen. Een vrij klassiek motief, financieel gewin, en een nieuwe vorm van een heel oud delict, namelijk oplichting of diefstal.

Onder gedigitaliseerde criminaliteit kan een veelheid van delicten vallen. Grofweg worden in de criminologische literatuur drie subcategorieën onderscheiden:

financieel-economische delicten, interpersoonlijke delicten en zedendelicten. Bij financieel-economische cyberdelicten is het doel van de daders financieel gewin. Voorbeelden hiervan zijn phishing, identiteitsfraude, WhatsAppfraude, koop- en verkoopfraude, diefstal, voorschotfraude, heling, CEO-fraude en datingfraude. Interpersoonlijke cyberdelicten zijn digitale vormen van strafbare gedragsdelicten waarbij de persoonlijke levenssfeer wordt aangetast. De meest voorkomende vormen zijn laster en chantage, gevolgd door stalking en bedreiging met geweld. Sinds de opkomst van het internet vinden zedendelicten ook online plaats. Voorbeelden hiervan zijn grooming en het verspreiden van kinderporno. Daarnaast zijn er de zogenaamde IBSA-delicten (*Image Based Sexual Abuse*), zoals het zonder toestemming verspreiden van naaktfoto's en -filmpjes (ook wel *shame sexting* genoemd) of hiermee dreigen (*sextortion*) (Powell et al., 2019). Zowel het dreigen met als het daadwerkelijk verspreiden van dergelijk seksueel beeldmateriaal zonder toestemming is strafbaar.

1.4 OVER EFFECTIEVE AANPAKKEN EN INTERVENTIES

De cyberweerbaarheid van eindgebruikers, organisaties en de samenleving vraagt om effectieve aanpakken en interventies. Het is daarom van belang om in kaart te brengen welke effecten en resultaten interventies behalen (Ooyen-Houben & Leeuw, 2010). Dankzij de toegenomen aandacht voor de thema's cyberweerbaarheid, cybersecurity en online criminaliteit zien we dat er veel interventies worden uitgevoerd. Maar een evaluatie van de effecten van deze interventies en aanpakken ontbreekt veelal. Ook zijn de interventies niet altijd ontwikkeld op basis van vooronderzoek onder de doelgroep en ontbreekt vaak een theoretische onderbouwing, oftewel interventies en aanpakken zijn vaak niet evidence-based (Bluhm et al., 2024). Leukfeldt (2024) roept daarom op om bij het versterken van de cyberweerbaarheid scherp oog te hebben voor (I) de onderbouwing en (II) het meten van de effecten van interventies om ervoor te zorgen dat we de